Resolución 304 EXENTA

APRUEBA EL TEXTO ACTUALIZADO Y REFUNDIDO DE LAS RECOMENDACIONES DEL CONSEJO PARA LA TRANSPARENCIA SOBRE PROTECCIÓN DE DATOS PERSONALES POR PARTE DE LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO Y SUSTITUYE TEXTO QUE INDICA

CONSEJO PARA LA TRANSPARENCIA

Fecha Publicación: 07-DIC-2020 | Fecha Promulgación: 30-NOV-2020
Tipo Versión: Única De : 07-DIC-2020
Url Corta: http://bcn.cl/2mn5i

APRUEBA EL TEXTO ACTUALIZADO Y REFUNDIDO DE LAS RECOMENDACIONES DEL CONSEJO PARA LA TRANSPARENCIA SOBRE PROTECCIÓN DE DATOS PERSONALES POR PARTE DE LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO Y SUSTITUYE TEXTO QUE INDICA

Núm. 304 exenta.- Santiago, 30 de noviembre de 2020.

Visto:

Lo dispuesto en la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la ley N°20.285; en el artículo 19 N°4 de la Constitución Política de la República; en la Ley N°19.628, sobre Protección de la Vida Privada; en el decreto con fuerza de ley N°1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.575, orgánica constitucional de bases generales de la Administración del Estado; en la Ley N°19.880, que establece Bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado; en el decreto supremo N°20, de 2009, del Ministerio Secretaría General de la Presidencia, que aprueba los Estatutos de Funcionamiento del Consejo para la Transparencia; en el acta de sesión ordinaria N°1.137, del Consejo Directivo del Consejo para la Transparencia, de fecha 15 de octubre de 2020; en la resolución exenta N°167, de 23 de abril de 2015, del Consejo para la Transparencia, que aprueba Reglamento de Suplencias y Subrogaciones del Consejo para la Transparencia, modificado por resolución exenta N°425, de 14 de agosto de 2019; en la resolución exenta N°127, de 3 de junio de 2020 del Consejo para la Transparencia, que aprobó la modificación del contrato de trabajo suscrita con don David Ibaceta Medina, designándolo Director Jurídico Titular de esta Corporación; y en la resolución exenta N°194, de 27 de agosto de 2020, del Consejo para la Transparencia, que designa a don David Ibaceta Medina, como Director General Suplente de esta Corporación.

Considerando:

a) Que, el numeral 4 del artículo 19 de la Constitución Política de la República asegura a todas las personas el derecho a la protección de datos personales y establece que el tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley.

b) Que, la Carta Fundamental reconoce explícitamente como derecho fundamental el derecho a la autodeterminación informativa, el cual se constituye ahora en un límite al ejercicio de la soberanía, en un deber de respeto y promoción por parte de los órganos del Estado y en una norma que delimita la acción de los órganos estatales, quienes deben someter su acción al nuevo derecho fundamental y a las normas dictadas conforme a la Constitución Política.

c) Que, el texto constitucional estableció, además, una reserva legal especial, en virtud de la cual el tratamiento y la protección de datos personales se realizará en la forma y condiciones que determine la ley. Esta reserva es especialmente relevante para los órganos del Estado, atendido el principio de legalidad o juridicidad en la actuación del Estado.

d) Que, la protección de datos personales se encuentra amparada, en el rango legal, por las disposiciones de la ley N°19.628, sobre Protección de la Vida Privada, que establecen las reglas generales sobre procesamiento de datos personales que realicen tanto los órganos de la Administración del Estado como particulares, determina un conjunto de derechos de los titulares y las obligaciones de los responsables del tratamiento, además de establecer una acción especial de tutela judicial de estos derechos, denominado habeas data.

e) Que, los procesos de recolección, procesamiento y transferencia de datos personales se han intensificado en la última década y el proceso de digitalización de la administración del Estado requerirá que dichas operaciones se incrementen de manera constante en el tiempo.

f) Que, las diversas medidas adoptadas por las autoridades sanitarias con ocasión de la pandemia por Covid-19, han demostrado la necesidad de actualizar las disposiciones de la ley y revisar la interpretación de algunos de sus preceptos, además de actualizar los criterios enunciados en las recomendaciones que se sustituyen.

g) Que, por lo anteriormente expuesto, el Consejo para la Transparencia estima necesario contribuir a elevar los estándares de protección de los datos personales en poder de los órganos de la Administración del Estado a fin de asegurar los derechos que la Constitución y las leyes reconocen a los titulares de los mismos.

h) Que, en esta materia, el literal m) del artículo 33 de la ley de transparencia de la función pública y de acceso a la información de la Administración del Estado, aprobada por el artículo primero de la Ley N°20.285, sobre Acceso a la Información Pública (en adelante, la "Ley de Transparencia") faculta al Consejo para velar por el debido cumplimiento de la ley N°19.628 por parte de los órganos de la Administración del Estado, que le habilitan a verificar la aplicación que los órganos públicos realicen de las disposiciones de esa ley, ya sea mediante la resolución de casos particulares o la dictación de recomendaciones, como la presente.

i) Que, además de velar por la protección de datos personales, desde la entrada en vigencia de la Ley de Transparencia, este Consejo, conociendo de reclamos por incumplimiento de los deberes de transparencia activa y de amparos por denegación de acceso a la información, se ha visto en la necesidad de interpretar el derecho de acceso a la información pública y el ahora derecho fundamental a la protección de datos personales, de manera armónica, lo que ha generado una abundante jurisprudencia al respecto.

j) Que, en virtud de la experiencia acumulada y en ejercicio de lo dispuesto en el literal m) del artículo 33 de la Ley de Transparencia se ha estimado conveniente proponer una serie de criterios que orienten la aplicación de las normas contenidas en la ley N°19.628 y que concreticen, además, el nuevo derecho fundamental a la protección de datos personales, todo ello con el objeto incrementar y mejorar el nivel cumplimiento de las obligaciones que la Constitución y la ley imponen a los órganos de la Administración del Estado en materia de protección de datos personales.

k) Que los principios de eficiencia y eficacia en la Administración del Estado obligan a las organizaciones del Estado a adoptar las medidas técnicas, administrativas y organizacionales necesarias en el cumplimiento de sus funciones públicas para, por una parte, gestionar adecuadamente sus sistemas de tratamiento de datos personales, y, por otra, garantizar una protección efectiva de los derechos de las personas. Una forma de implementar estos principios -conforme la experiencia comparada muestra- implica adoptar el enfoque de protección de datos personales por diseño en los sistemas de tratamiento de datos personales cuyos responsables sean órganos de la Administración del Estado.

l) Que el tratamiento de datos personales que realizan los órganos de la

Administración del Estado en sistemas basados en tecnologías digitales genera nuevos riesgos y amenazas para la confidencialidad, integridad y disponibilidad de la información, los cuales deben ser identificados, mitigados y administrados bajo las directrices de la gestión de riesgos. En este sentido, los órganos de la Administración del Estado deben implementar las medidas de seguridad en el tratamiento de datos personales propuestas en la Política Nacional de Ciberseguridad y en los instructivos presidenciales sobre ciberseguridad, toda vez que su correcta aplicación puede contribuir a mitigar esos nuevos riesgos y amenazas.

m) Que la Ley N°21.180 sobre Transformación Digital del Estado introdujo una serie de modificaciones a las reglas sobre procedimiento administrativo, con el fin de avanzar hacia la digitalización de la gestión administrativa del Estado, mediante la comunicación electrónica entre órganos de la Administración del Estado, el establecimiento de procedimientos administrativos electrónicos, la digitalización de documentos, la notificación electrónica y la implementación del principio de interoperabilidad, las que comenzarán a entrar en vigencia a partir a mediados del año 2021 hasta su total implementación en el año 2024.

n) Que, en razón de lo anterior, el Consejo Directivo del Consejo para la Transparencia, en sesión ordinaria N°1.137, de fecha 15 de octubre de 2020, acordó por unanimidad, aprobar las modificaciones a las recomendaciones dictadas el año 2011, lo que se materializará a través de la presente resolución que, para los efectos de una adecuada comprensión de las mismas, procederá a actualizar y refundir, tanto las nuevas disposiciones, como aquellas que forman parte de las recomendaciones vigentes hasta la fecha, procediendo en definitiva, a sustituir dicho texto.

Resuelvo:

1° Apruébase el texto refundido y actualizado de las Recomendaciones sobre Protección de Datos Personales por parte de los Órganos de la Administración del Estado:

RECOMENDACIONES DEL CONSEJO PARA LA TRANSPARENCIA SOBRE PROTECCIÓN DE DATOS PERSONALES POR PARTE DE LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO

1. OBJETO DE LAS RECOMENDACIONES.

Las presentes Recomendaciones tienen por objeto orientar la aplicación concreta del nuevo derecho fundamental a la protección de datos personales, además de entregar criterios jurídicos a los órganos de la Administración del Estado en el tratamiento de datos personales que realicen dentro del ámbito de sus competencias, a fin de dar cumplimiento a las obligaciones legales que éstos tienen como responsables de tratamiento, conforme a lo dispuesto en la ley N°19.628 y en las demás normas pertinentes.

2. ÁMBITO DE APLICACIÓN DE LAS RECOMENDACIONES.

Las Recomendaciones serán aplicables al tratamiento de datos personales que efectúen los órganos de la Administración del Estado, entendiendo por tales los comprendidos en el inciso primero del artículo 2° de la Ley de Transparencia.

Las Recomendaciones serán aplicables tanto al tratamiento de datos personales que se realice dentro del territorio nacional como a aquellos que se verifiquen extraterritorialmente mediante prestadores de servicios de alojamiento o procesamiento de datos, incluyendo servicios cloud o en la nube. Asimismo, se aplicarán a las eventuales transferencias internacionales de datos personales que realicen organismos públicos en cumplimiento de algún mandato legal.

3. DEFINICIONES PREVIAS.

Para efectos de la aplicación de estas Recomendaciones deberán considerarse las definiciones contenidas en el artículo 2 de la Ley N°19.628, sobre Protección de la Vida Privada, y, especialmente, se entenderá por:

3.1. Datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables, ya sea que se trate de información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, no importando el soporte en el que conste.
Por tanto, los elementos básicos de la definición son:

i. Debe tratarse de información relativa a una persona natural.
ii. Debe tratarse de información que permita identificar al titular. Se entiende para estos efectos por identificable, toda persona cuya identidad pueda determinarse, directa o indirectamente, por ejemplo, mediante uno o más elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social, siempre y cuando el esfuerzo de determinación no resulte excesivo o desproporcionado.
iii. El titular sólo puede ser una persona natural.

3.2. Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
3.3. Registro o banco de datos, el conjunto organizado de datos de carácter personal sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.
3.4. Responsable del registro o banco de datos, el organismo público que realiza el tratamiento de datos personales dentro del ámbito de sus competencias y para el cumplimiento de sus funciones legales, ya sea que lo realice por sí mismo, o a través de un encargado.
3.5. Tratamiento de datos, cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma. Estas operaciones pueden ser realizadas directamente por el responsable del registro o, también, por el encargado del tratamiento.
3.6. Encargado de tratamiento, aquella persona natural o jurídica que realiza un tratamiento de datos por encargo o mandato del responsable de la base de datos, al que le serán aplicables las reglas generales en la materia. También se le denomina mandatario. El mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos, y el mandatario estará obligado a respetar esas estipulaciones en el cumplimiento de su encargo.
3.7. Fuentes accesibles al público, los registros de datos personales, públicos o privados, que están permanentemente a disposición del público y cuya consulta puede ser realizada por cualquier persona.
3.8. Dato caduco, el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.
3.9. Dato estadístico, el dato que en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.
3.10. Disociación de datos, el procedimiento que se realiza para desvincular un conjunto de datos personales, de manera irreversible, de una persona determinada o determinable.

4. PRINCIPIOS ORIENTADORES DE LA PROTECCIÓN DE DATOS.
Los principios orientadores de la protección de datos que informan su tratamiento por parte de los organismos de la Administración del Estado son los siguientes: licitud, calidad, información, seguridad, confidencialidad y especial protección de datos personales sensibles.

4.1. Principio de licitud. De conformidad con la constitucionalización del derecho a la protección de datos personales, que establece una reserva legal especial en virtud de la cual el tratamiento y la protección de datos personales se podrá realizar en la forma y condiciones que establezca la ley, el artículo 4 de la ley N°19.628, señala que sólo es posible tratar datos de carácter personal cuando exista autorización legal, ya sea de la propia ley N°19.628 o de otras normas de igual rango.

En el caso de los órganos de la Administración del Estado, la habilitación legal genérica para el tratamiento de datos personales se encuentra contenida en el artículo 20 de la ley N°19.628, que permite a los órganos públicos realizar tratamiento de datos personales solo respecto de las materias de su competencia y con sujeción a las reglas de los artículos 1 al 19 de la misma ley, entre las cuales se encuentran los principios de licitud, finalidad, calidad, responsabilidad y seguridad, junto con los deberes de información y especial protección de los datos personales sensibles, además de permitir el ejercicio de los derechos de los titulares.

4.2. Principio de calidad de los datos. Este principio consiste en que los datos tratados deben ser exactos, adecuados, pertinentes y no excesivos, y deberá ser observado durante la recogida y posterior tratamiento de los datos, incluyendo la purga o eliminación. Concurren, por tanto, tres principios rectores:

a) Principio de veracidad. De conformidad con el inciso segundo del artículo 9° de la ley N°19.628, los datos personales deben ser exactos, actualizados y responder con veracidad a la situación real de su titular. Por consiguiente, el organismo público responsable de la base de datos deberá, sin necesidad de requerimiento del titular, eliminar los datos caducos y aquellos que estén fuera de su competencia; bloquear los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda su cancelación; y modificar los datos inexactos, equívocos o incompletos.

b) Principio de finalidad. Según lo dispone el inciso primero del artículo 9° de la ley N°19.628, los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados. La referida finalidad, en el caso de órganos de la Administración del Estado, estará determinada en función de las materias propias de su competencia y por la función legal específica que está ejecutando y que justifica el procesamiento de datos personales.

c) Principio de proporcionalidad. Este principio, que es aplicación de los principios de eficiencia, eficacia e idónea administración de los medios que deben observar los órganos de la Administración del Estado, implica que sólo pueden recabarse aquellos datos que sean necesarios para conseguir los fines que justifican su recolección. Por tanto, se entenderá que se cumple con el principio de proporcionalidad cuando: el o los datos que se recolecten, así como su posterior tratamiento, sean adecuados o apropiados a la finalidad que lo motiva; sean pertinentes o conducentes para conseguir la referida finalidad y no excesivos en relación con dicha finalidad para la cual se han obtenido, en el sentido que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia. En aplicación de este principio, los órganos o servicios públicos deberán optar, de entre los diversos tratamientos que les permitan conseguir los fines pretendidos dentro del ámbito de sus competencias, por aquel que menor incidencia tenga en el derecho a la protección de datos personales y por la utilización de los medios menos invasivos.

4.3. Deber de información. De acuerdo con lo dispuesto en los artículos 3°, 4° y 20 de la ley N°19.628, los organismos públicos están obligados a informar a su titular acerca de la identidad del órgano responsable de la base de datos, de la finalidad perseguida con el tratamiento de la información, de la posible comunicación a terceros y de los derechos que pueden ser ejercidos por ellos.

4.4. Principio de seguridad. Conforme a lo establecido en el artículo 11 de la ley N°19.628, el responsable de los registros o bases donde se almacenen datos personales, con posterioridad a su recolección, deberá cuidar de ellos con la

debida diligencia, haciéndose responsable de los daños. Por tanto, los órganos de la Administración del Estado, a fin de dar cumplimiento a lo anterior, deben aplicar medidas de seguridad, técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información.

Asimismo, respecto de la seguridad y confidencialidad de los documentos electrónicos, deben aplicar estrictamente las disposiciones del decreto supremo N°83, de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la Administración del Estado, sobre seguridad y confidencialidad de los documentos electrónicos.

Finalmente, los organismos públicos deben implementar las medidas pertinentes de la Política Nacional de Ciberseguridad y los Instructivos Presidenciales que imponen medidas específicas sobre ciberseguridad que deben observar los órganos de la administración del Estado.

4.5. Principio de confidencialidad o secreto. Según lo prescribe el artículo 7° de la ley N°19.628, las personas que trabajan en el tratamiento de datos personales o tengan acceso a éstos de otra forma (como aquellos funcionarios públicos autorizados para el acceso a bancos de datos de los organismos respectivos), están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo.

4.6. Deber de protección especial de los datos personales sensibles. Conforme prescribe el artículo 10 de la ley N°19.628, existe una prohibición general de tratamiento de datos personales sensibles, salvo cuando una disposición legal lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

De esta manera, únicamente los organismos de la Administración del Estado que cumplan con alguna de esas condiciones expresas podrán realizar tratamiento de datos personales sensibles, sobre los cuales deberán adoptar medidas de seguridad adecuadas al nivel de sensibilidad y riesgo de los datos tratados.

5. DERECHOS DE LOS TITULARES DE DATOS PERSONALES.

Los titulares de datos personales, conforme a lo establecido en el artículo 12 de la ley N°19.628, pueden ejercer respecto de los órganos de la Administración del Estado, los derechos que se describen en este numeral, teniendo presente las características de independencia, gratuidad y sencillez y las recomendaciones que en cada caso se señalan a continuación.

5.1. Derecho a acceder a sus propios datos. Toda persona tiene derecho a exigir del órgano o servicio que sea responsable de un banco, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

En este caso la información será entregada en forma gratuita, no siendo posible siquiera cobrar los costos directos de reproducción de esa información. Si los datos personales están en una base de datos a la que tienen acceso diversos organismos, el titular podrá requerir información a cualquiera de ellos.

Cuando en el ejercicio del derecho de acceso a la información pública establecido en la Ley de Transparencia se soliciten antecedentes que, obrando en poder de la Administración, contengan datos personales de los que es titular el solicitante, se aplicará el procedimiento establecido en dicha ley, incluyendo la posibilidad de recurrir de amparo ante este Consejo, de conformidad a lo dispuesto en el artículo 24 y siguientes de la Ley de Transparencia. No obstante, en lo relativo a la gratuidad del acceso, se observará lo dispuesto en la ley N°19.628.

5.2. Derecho de rectificación o modificación. Toda persona tiene derecho a exigir que los datos que sean erróneos, inexactos, equívocos o incompletos, se modifiquen, siempre que se acredite debidamente cualquiera de dichas circunstancias y se indique con claridad la corrección solicitada. Lo anterior, es sin perjuicio de

la rectificación o modificación de oficio por parte del órgano o servicio público, en aplicación directa de los principios de calidad de los datos y de idónea administración de los medios del Estado.

5.3. Derecho de cancelación o eliminación. Toda persona tiene derecho a exigir que se eliminen aquellos datos cuyo almacenamiento carece de fundamento legal o se encuentran caducos, salvo que concurra alguna excepción legal, como es el caso de lo dispuesto en el artículo 15 de la ley N°19.628.

Las solicitudes de rectificación y cancelación serán gratuitas debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Los órganos o servicios públicos no estarán autorizados a cobrar los costos directos de reproducción por la entrega de dicha información. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que hayan transcurrido, a lo menos, seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita podrá ejercerse personalmente por el titular del dato o debidamente representado.

Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el órgano deberá comunicarles, a la brevedad posible, la operación efectuada. Si no fuere posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos. De todo ello deberá informarse, oportunamente y por escrito, al titular del dato.

5.4. Derecho al bloqueo de datos. Es el derecho a exigir la suspensión temporal de cualquier operación de tratamiento de los datos almacenados. Procede en los casos determinados en el inciso cuarto del artículo 12 de la ley N°19.628, cuando el titular ha proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones informativas y no desee continuar figurando en el registro respectivo de modo temporal o definitivo. También procede en los casos del inciso tercero del artículo 6°, de la norma legal antes señalada, cuando la exactitud de los datos personales no pueda ser establecida o cuya vigencia sea dudosa y respecto a los cuales no corresponda la cancelación. Lo anterior, es sin perjuicio de lo dispuesto en este instrumento, en materia de límites al ejercicio de los derechos.

6. PROCEDIMIENTO Y FORMULARIO PARA EL EJERCICIO DE LOS DERECHOS.

Para facilitar el ejercicio de los derechos señalados en los numerales precedentes, los órganos de la Administración del Estado podrán disponer de procedimientos y formularios simplificados, los cuales deben estar disponibles en cada una de las Oficinas de Información, Reclamos y Sugerencias, como también en sus respectivas páginas web. En los referidos formularios se exigirá:

a) El nombre y apellidos del titular de los datos y una forma de verificación de la identidad que no implique reproducir documentos de identidad ni generar nuevos procesamientos de datos personales.

b) La dirección del solicitante a efectos de notificación, la que podrá ser, indistintamente, una dirección de correo electrónico o una postal.

c) El derecho que se ejerce.

d) La fecha y la firma del solicitante, estampada por cualquier medio habilitado.

e) Los documentos acreditativos de la solicitud, en caso de ser procedente.

Si se establece un procedimiento en línea para el ejercicio de derechos, deberá utilizarse un mecanismo de autenticación idóneo y seguro, como Clave Única o similares, que garanticen la confidencialidad, disponibilidad e integridad de la información transmitida, cumpliendo además con el deber de información y el principio de seguridad que establece la ley N°19.628.

6.1. Ejercicio independiente. Cada uno de los derechos de los titulares de datos personales podrán ser ejercido en forma independiente, es decir, no puede exigirse el ejercicio de ninguno de ellos como condición o requisito previo para el ejercicio

del otro.

6.2. Ejercicio a través de apoderado. El ejercicio de derechos señalados previamente podrá realizarse de manera personal o mediante apoderado. En este último caso, el apoderado tendrá las mismas facultades que el titular del dato, salvo manifestación expresa en contrario.

El mandato o poder podrá constar en un documento suscrito mediante firma electrónica simple o avanzada, en escritura pública o en documento privado suscrito ante notario, y deberá contener toda la información necesaria para el ejercicio de los derechos.

6.3. Ejercicio de los derechos ante el encargado o mandatario. En caso de que el organismo de la Administración del Estado hubiese encargado el tratamiento de los datos a un tercero, los titulares de éstos podrán ejercer sus derechos directamente ante él o ante el órgano o servicio, a su elección. En el contrato respectivo deberá establecerse la forma en que se dará respuesta en estos casos, buscando en todo momento responder en forma oportuna y adecuada al titular del dato.

6.4. Prohibición de limitación. Los derechos de los titulares de datos personales no podrán ser limitados por los órganos de la Administración del Estado, por medio de ningún acto o convención.

6.5. Límites al ejercicio de los derechos. Sin perjuicio de lo dispuesto en los numerales precedentes, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando:

i. Ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo de la Administración del Estado requerido;

ii. Afecte la reserva o secreto establecidos en disposiciones legales, las que, de acuerdo con el inciso 2° del artículo 8° de la Constitución Política de la República, deberán tener rango de ley de quórum calificado. En especial, cuando se configure algunas de las causales establecidas en el artículo 21 de la Ley de Transparencia;

iii. Afecte la seguridad de la Nación;

iv. Afecte el interés nacional; o,

v. Hubiesen sido almacenados por mandato legal. En este caso, el mandato legal deberá ser expreso y autorizar al órgano o servicio para hacer tratamiento de datos respecto de un determinado banco de datos. La procedencia de la modificación, cancelación o bloqueo de los datos en esos casos estará sometida y tendrá el alcance que establezca la normativa respectiva.

6.6. Obligación de evacuar respuesta. El órgano o servicio público estará obligado a evacuar respuesta a la solicitud efectuada por el titular de los datos, en el plazo de dos días hábiles que establece el artículo 16 de la ley N°19.628, aunque no disponga de los datos de carácter personal de la persona que ejerció el derecho.

6.7. Plazo de respuesta y efectos de la falta de pronunciamiento en tiempo o de la denegación. Si el órgano o servicio responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, solicitando amparo a los derechos consagrados en este numeral, de acuerdo al procedimiento establecido en el inciso segundo del artículo 16 de la ley N°19.628.

En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia.

El procedimiento ante la Corte Suprema se someterá a las normas establecidas en los incisos tercero y siguientes del artículo 16 de la ley N°19.628.

7. OBLIGACIONES ESPECÍFICAS DE LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO.

7.1. Condiciones de licitud en el tratamiento de los datos. La habilitación legal genérica de tratamiento de datos personales de los órganos de la Administración del Estado está contenida en el artículo 20 de la ley N°19.628, que permite a dichos órganos públicos a realizar tratamiento de datos personales solo respecto de las materias de su competencia y con sujeción a las reglas de los artículos 1 al 19 de la misma ley, entre las cuales se encuentran los principios de licitud, finalidad, calidad, responsabilidad y seguridad, junto con los deberes de información y especial protección de los datos personales sensibles, además de permitir el ejercicio de los derechos de los titulares.

Eventualmente, un órgano de la Administración del Estado podría realizar tratamiento de datos personales obteniendo el consentimiento del titular de los datos siempre y cuando sea por aplicación de los principios de eficiencia o eficacia o por la naturaleza del tratamiento o la prestación pública que está realizando. En este caso, el órgano deberá además dar aplicación estricta a lo dispuesto en el artículo 4° de la ley N°19.628, es decir el consentimiento deberá constar por escrito y podrá ser revocado por el titular de los datos personales. Con todo, el tratamiento deberá realizarse dentro del ámbito de sus competencias.

7.2. Requerimientos para el tratamiento de datos. Los órganos o servicios públicos deben sujetarse para el tratamiento de los datos, según el artículo 20, a las reglas establecidas en la ley N°19.628. En consecuencia:

a) Los órganos de la Administración del Estado deben informar al titular de los datos, según lo dispone el artículo 4° de la ley N°19.628, el propósito del almacenamiento de sus datos personales, es decir, la finalidad perseguida con el tratamiento de la información, y la posible comunicación a terceros. De la misma forma, se debe informar al titular, la denominación del órgano o servicio responsable del tratamiento de la base de datos y los derechos que le asisten para la protección de sus datos personales.

Se recomienda especialmente a los órganos o servicios públicos que dispongan de una política proactiva de difusión de información en esta materia a fin de dar cabal cumplimiento al deber de informar antes señalado.

Conforme lo anterior y sin perjuicio de los mecanismos especiales dispuestos por cada órgano de la Administración del Estado, podrán contemplar dichos antecedentes en la Política de Protección de Datos Personales poniéndola a disposición permanente del público en los respectivos sitios web institucionales, mediante afiches; o la mención a tal política en los formularios en que se soliciten datos personales (formulario de registro), señalando dónde se encuentra ésta, entre otras.

b) Los órganos o servicios públicos deberán necesariamente, de conformidad al artículo 9° de la ley N°19.628, efectuar el tratamiento de los datos personales cumpliendo con las finalidades correspondientes a las materias de su competencia. Se recomienda que estas finalidades se encuentren explicitadas, a modo ejemplar, en la Política de Protección de Datos Personales, en los formularios de registro, formulario papel u otro medio, para de esta manera informar adecuadamente a su titular.

c) En virtud del principio de calidad de los datos y de los artículos 6° y 9°, inciso segundo, de la ley N°19.628 y los principios de eficiencia, eficacia e idónea administración de los medios públicos contenidas en el artículo 3° y 5° del decreto con fuerza de ley N°1/19.653, de 2000 del Ministerio Secretaría General de la Presidencia, que fija texto refundido, coordinado y sistematizado de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, los órganos o servicios públicos deberán de oficio y sin necesidad de requerimiento del titular de los datos: eliminar los datos caducos y aquellos que se encuentren fuera de su competencia por carecer de fundamento legal; bloquear los datos cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación; y modificar los datos inexactos, equívocos o incompletos.

d) En virtud del principio de seguridad y de lo dispuesto en el artículo 11 de

la ley N°19.628, los órganos o servicios públicos deberán adoptar todas las medidas, tanto organizativas como técnicas, para resguardar la integridad, confidencialidad y disponibilidad de los datos contenidos en sus registros con la finalidad de evitar su alteración, pérdida, transmisión y acceso no autorizado, haciéndose responsable de los daños causados. En este sentido, los organismos públicos deberán aplicar diversos niveles de seguridad atendiendo al tipo de dato almacenado, conforme se traten, por ejemplo, de datos personales sensibles, respecto de los cuales deben adoptarse niveles de seguridad más altos en comparación con aquellos que no posean dicha calidad.

Respecto de la seguridad y confidencialidad de los documentos electrónicos, deben aplicar estrictamente las disposiciones del decreto supremo N°83, de 2004, del Ministerio Secretaría General de la Presidencia, que aprobó la Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos.

e) Los órganos o servicios públicos deberán exigir a sus funcionarios cumplir con la obligación de secreto o confidencialidad en relación a los datos que provengan o hayan sido recolectados de fuentes no accesibles al público, contemplada en el artículo 7° de la ley N°19.628, en especial respecto de los que trabajen en el tratamiento de datos personales o tengan acceso a éstos de cualquier otra forma, extendiéndose, igualmente, este deber a los demás datos o antecedentes relacionados con el banco de datos, como por ejemplo respecto de las medidas de seguridad adoptadas a su respecto. Asimismo, la referida obligación del funcionario público no cesará por haber terminado sus obligaciones en ese campo, es decir, por dejar de desempeñarse en el tratamiento o acceso a dichos registros o en el Servicio mismo.

f) Los órganos o servicios públicos deberán formar, capacitar y entrenar a sus funcionarios en el cumplimiento de las disposiciones de la ley N°19.628 y respecto del nuevo derecho fundamental a la protección de datos personales, de manera de cumplir con el mandato constitucional de promover y proteger efectivamente los derechos consagrados en la Constitución y en los tratados internacionales ratificados por Chile y que se encuentren vigentes.

8. REGLAS ESPECIALES PARA EL TRATAMIENTO DE DATOS PERSONALES SENSIBLES POR PARTE DE LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO.

La ley N°19.628 identifica una categoría especial de datos personales denominados datos sensibles, que son aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Al tratarse de una definición legal de carácter abierto, el concepto de dato personal sensible puede abarcar aspectos disímiles entre sí. Por ello, los órganos de la Administración del Estado deben tener presente, al menos, las siguientes categorías de datos personales sensibles:

i. Datos que se refieren a características físicas de una persona, tales como datos biométricos, muestras y datos biológicos, datos de salud ya sea física, psíquica, entre otros.

ii. Datos que se refieren a características morales de una persona, tales como información sobre orientación o preferencia sexual, creencias o convicciones religiosas, éticas o políticas, entre otros.

iii. Datos que se refieren a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, la información sobre desplazamiento geográfico, la geolocalización, la navegación en internet, entre otros.

Conforme prescribe el artículo 10 de la ley N°19.628, existe una prohibición general de tratamiento de datos personales sensibles salvo cuando una disposición legal lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

De esta manera, únicamente los organismos de la Administración del Estado que cumplan con alguna de esas condiciones expresas podrán realizar tratamiento de datos personales sensibles.

Respecto de la autorización legal, cada organismo público debe examinar si cuenta con habilitación legal expresa en las normas que regulan su funcionamiento, establezcan sus competencias o determinen sus funciones especiales. De ser así, el tratamiento de datos personales sensibles tendrá su fundamento legal en esa regla expresa.

En aquellos casos donde no exista tal regla expresa, el tratamiento de datos personales sensibles podría basar su habilitación legal en la regla general del artículo 20 de la ley N°19.628, si y solo si el tratamiento de esta categoría especial de datos resulta imprescindible para el debido cumplimiento de su función pública, forme parte esencial de las materias de su competencia y se efectúe con pleno respeto a las reglas contenidas entre los artículos 1° y 19 de la ley N°19.628, conforme detalladamente se analiza previamente. En ausencia de esa autorización legal, los organismos de la Administración del Estado no podrán tratar datos personales sensibles, a menos que obtengan consentimiento expreso del titular o que sea necesario para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares de dichos datos.

Respecto del consentimiento, si un organismo de la Administración del Estado requiere tratar datos personales sensibles y no cuenta con la habilitación legal antes mencionada, podrá hacerlo obteniendo el consentimiento previo y expreso del titular, en los términos establecidos en el artículo 4° de la ley N°19.628, cumpliendo además de manera estricta con lo dispuesto en el artículo 20 de la misma ley que establece que ese tratamiento "sólo podrá efectuarse respecto de las materias de su competencia" e informando adecuadamente sobre la finalidad de la captura de datos, su procesamiento y eventual comunicación.

Finalmente, respecto a la determinación u otorgamiento de beneficios de salud, el artículo 10 de la ley N°19.628 establece una regla especialísima respecto del tratamiento de datos personales sensibles cuando sean necesarios para la determinación u otorgamiento de beneficios de salud para el titular. En el caso de organismos públicos, la aplicación de esta regla tiene un alcance limitado, toda vez que únicamente podrán hacer uso de esta disposición aquellos organismos públicos que otorguen "beneficios de salud" en el ejercicio de sus funciones y respecto de materias de su competencia, conforme dispone el artículo 20 de la ley N°19.628.

9. TRATAMIENTO DE DATOS PERSONALES RELATIVOS A DELITOS, INFRACCIONES ADMINISTRATIVAS O FALTAS DISCIPLINARIAS.

Los órganos de la Administración del Estado, conforme a lo dispuesto en el artículo 21 de la ley N°19.628, que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena.

Se exceptuarán de la prohibición de comunicación, los casos en que esa información les sea solicitada por los Tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia, quienes deberán guardar respecto de ella la debida reserva o secreto y, en todo caso, les serán aplicables los siguientes artículos de la ley N°19.628:

a) El artículo 5° que regula el procedimiento automatizado de transmisión de datos,

b) El artículo 7° que consagra el principio de secreto exigible a los funcionarios públicos,

c) El artículo 11 que establece el principio de seguridad y

d) El artículo 18 referido a la prohibición de comunicación de datos personales relativos a obligaciones de carácter económico, financiero bancario o comercial cuando han transcurrido cinco años desde que la obligación se hizo exigible, después de haber sido pagada o haberse extinguido la obligación por otro

modo legal, sin perjuicio de la comunicación a los Tribunales de Justicia de la información que requieran con motivo de juicios pendientes.

10. INSCRIPCIÓN DE LAS BASES DE DATOS EN EL REGISTRO DE BANCOS DE DATOS PERSONALES A CARGO DE ORGANISMOS PÚBLICOS.

Los órganos de la Administración del Estado deberán inscribir todos los bancos de datos personales que obren en su poder en el Registro de los Bancos de Datos Personales a cargo de Organismos Públicos que lleva el Servicio de Registro Civil e Identificación, de acuerdo a lo establecido en el artículo 22 de la ley N°19.628, en el decreto supremo N°779, de 2000, del Ministerio de Justicia, que aprobó el Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos y en la resolución (E) N°1.540, de 2010, del Servicio de Registro Civil e Identificación.

10.1. Características del registro. Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, eI fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende.

10.2. Requisitos de la inscripción. Conforme a la normativa aludida, el organismo público responsable del banco de datos para efectos de la inscripción debe proporcionar, a lo menos:

i. El nombre del banco de datos personales, es decir, la denominación que eI propio organismo le dé al banco de datos que inscriba y que sirva para su identificación;

ii. El organismo público responsable del banco de datos personales respectivo;

iii. El RUT correspondiente al organismo público;

iv. El fundamento jurídico de la existencia del banco de datos personales, es decir, se deben indicar las normas legales que sancionan en forma específica la existencia de un registro en particular, o las normas de carácter general, sectorial u orgánica que habiliten al organismo público para tratar los datos personales y almacenarlos en bancos de datos;

v. La finalidad del banco de datos;

vi. El o los tipos de datos almacenados en dicho banco, pudiendo corresponder, a cualquiera de las siguientes categorías de datos: biométricos, civiles, económicos y financieros, generales, judiciales o legales, de salud, sociales y otros datos referidos a cualquier otra información concerniente a personas naturales, identificadas o identificables, almacenada en la base de datos del organismo respectivo; y

vii. Una descripción del universo de personas que comprende.

10.3. Procedimiento de inscripción. El procedimiento de inscripción de los bancos de datos personales a cargo de los órganos de la Administración del Estado se encuentra regulado en el decreto supremo N°779, de 2000, del Ministerio de Justicia, que aprobó el Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos y en las resoluciones que el Director Nacional estime pertinente dictar al efecto, en especial, la resolución (E) N°1.540, de 2010, que establece el procedimiento de inscripción de registros y/o bancos de datos personales a cargo de los organismos públicos o la que la reemplace.

10.4. Oportunidad de la inscripción. Los órganos o servicios públicos deberán inscribir la base de datos dentro del plazo de 15 días contados desde que se inicien las actividades del respectivo banco.

10.5. Correcciones de la inscripción. Cualquier corrección relativa a errores u omisiones de una inscripción deberá ser requerida por el propio organismo responsable de dicha inscripción en el Registro de Bancos de Datos Personales, siguiendo el mismo procedimiento establecido para la inscripción.

10.6. Modificaciones de la inscripción. Cualquier modificación de una inscripción deberá ser requerida por el propio organismo responsable de la inscripción en el Registro de Bancos de Datos Personales, en el plazo de 15 días

contados desde que se produzca cualquier cambio en la información proporcionada, de acuerdo con lo establecido en el numeral 10.2 anterior.

11. COMUNICACIÓN O TRANSMISIÓN DE DATOS PERSONALES.

Los organismos de la Administración del Estado solo podrán establecer procedimientos de comunicación, transmisión o cesión de datos de carácter personal para fines que digan directa relación con sus competencias legales y las de los organismos participantes, respecto del ejercicio de funciones específicas contenidas en sus respectivas leyes orgánicas o en otras disposiciones legales que expresamente los faculten para tales efectos, aplicando además los principios orientadores establecidos en estas recomendaciones.

El receptor sólo podrá utilizar los datos personales para los fines que motivaron la transmisión. Dicho procedimiento podrá contemplar las siguientes etapas: requerimiento expreso, admisibilidad de este y firma de un convenio de transmisión, las que se someterán a los lineamientos que se señalan a continuación.

El requerimiento de datos personales efectuado a un órgano o servicio público contendrá las siguientes especificaciones:

a) La individualización del requirente, el que puede ser un organismo público o privado, con indicación expresa de la habilitación legal para el tratamiento que invoque. En el caso de los organismos públicos, deberán identificar la función legal específica que se está ejecutando y que requiere de la comunicación o transferencia de datos personales.

b) El motivo y el propósito del requerimiento, con indicación expresa del tratamiento de datos que se busque efectuar y la finalidad del mismo, y

c) El tipo de datos que se desea transmitir, con indicación expresa de la pertinencia o necesidad de los datos solicitados en relación con las finalidades informadas.

La admisibilidad del requerimiento será evaluada por el órgano o servicio responsable del banco de datos que lo recibe, verificando que la comunicación guarde relación con sus tareas o finalidades, es decir, que se encuentra dentro del ámbito de sus competencias, y estableciendo los requisitos necesarios para el resguardo de los derechos de protección de datos en el convenio respectivo.

De la transmisión, la fecha, el motivo y propósito de la misma, los requisitos específicos para la protección de los datos personales transmitidos y la obligación del solicitante de utilizar los datos personales sólo para los fines que motivaron la transmisión se dejará constancia en un convenio de comunicación o transmisión suscrito por ambas partes, el que se entenderá aprobado una vez que se encuentre totalmente tramitado el o los correspondientes actos administrativos de aprobación, según se trate de uno o más órganos públicos. Por tanto, a lo menos deberá contener:

i. Identificación del órgano público que transmite los datos y del destinatario de estos,

ii. Identificación del banco de datos, según la denominación dada en la inscripción efectuada en el Registro de Bancos de Datos Personales a cargo de Organismos Públicos,

iii. Las medidas de seguridad que deberán adoptar tanto el que transmite los datos como el destinatario de estos durante todo el procedimiento de transmisión y posterior tratamiento de los datos por este último,

iv. La indicación de que el receptor de los datos tendrá la calidad de responsable del tratamiento, estando sometido a las mismas obligaciones, multas y responsabilidad de indemnizar en caso de tratamiento indebido de los datos, que el órgano público que efectuó la transmisión,

v. El procedimiento para efectuar el aviso a que se refiere el artículo 12, inciso final, de la ley N°19.628, en caso de que se ejerza ante cualquiera de los responsables de la base de datos comunicada los derechos de modificación,

cancelación o bloqueo, adoptando las medidas de trazabilidad que correspondan,

vi. El plazo que el destinatario conservará los datos transmitidos, y

vii. Los cursos de acción que deberá seguir el destinatario una vez que haya efectuado el tratamiento que motivó la transmisión, ya sea que se acuerde la destrucción o devolución del banco de datos al transmisor y de cualquier otro soporte donde consten los datos objeto de la comunicación.

No serán aplicables las recomendaciones contenidas en este numeral a los convenios o contratos celebrados entre órganos o servicios públicos y particulares cuando este último tenga la calidad de encargado del tratamiento, esto es, cuando actúa bajo las instrucciones del organismo responsable del tratamiento, caso en el cual, deberá estarse a las exigencias contempladas en el mandato.

Tampoco serán aplicables las recomendaciones contenidas en este numeral, a las comunicaciones o transferencias de datos personales que se realicen de conformidad a lo dispuesto en el artículo 24 bis de la ley N°19.880, sobre remisión electrónica de documentos o información entre organismos públicos para la sustanciación de un procedimiento administrativo electrónico1.

12. TRATAMIENTO DE DATOS A TRAVÉS DE UN ENCARGADO.

Los órganos o servicios públicos, en conformidad a lo dispuesto en eI artículo 8° de la ley N°19.628, podrán encargar el tratamiento de los datos a un tercero, que tendrá la calidad de encargado o mandatario.

El contrato de prestación de servicios de tratamiento que encargue el tratamiento de datos personales deberá ser otorgado por escrito y deberá contener al menos las siguientes menciones:

a) Que el tratamiento se efectúa a cuenta y riesgo del organismo responsable del tratamiento,

b) Los tipos de datos personales y las condiciones de utilización de los datos,

c) Las medidas de seguridad que se deban adoptar,

d) Las exigencias de confidencialidad de las personas que trabajen en el tratamiento y, en general, de la necesidad de dar cumplimiento a las obligaciones establecidas en la ley N°19.628 y de observar las presentes recomendaciones,

e) El plazo que el encargado conservará los datos y las condiciones para su devolución o eliminación segura e irrevocable. Los órganos públicos deberán adoptar las medidas técnicas y contractuales necesarias para impedir cualquier procesamiento de datos personales por parte del encargado, una vez terminado el contrato suscrito.

En estos casos no se entenderá que existe transmisión, comunicación o cesión de datos entre el responsable del tratamiento y el encargado.

Las mismas menciones señaladas previamente deberán contener las contrataciones de bienes y servicios que se realicen en un proceso de contratación pública regido por la Ley N°19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios. En este caso, el órgano de la administración del Estado licitante deberá incorporar desde el diseño de las bases administrativas y técnicas de los convenios que involucren -o puedan involucrar- operaciones de tratamiento de datos personales, las menciones señaladas en los literales anteriores y deberán adoptar las medidas que sean necesarias para el cumplimiento integral de las disposiciones contenidas en el artículo 8° de la ley N°19.628.

Igual obligación recaerá en la Dirección de Compras y Contratación Pública al momento de diseñar las bases técnicas y administrativas de las licitaciones para la contratación de bienes y servicios a través de la modalidad de convenios marco, regulados en el literal d) del artículo 28 de la ley N°19.886.

13. MEDIDAS DE SEGURIDAD DE LOS BANCOS O REGISTROS DE DATOS.

En virtud del principio de seguridad y de lo dispuesto en el artículo 11 de la ley N°19.628, los organismos de la Administración del Estado deben adoptar todas las medidas, tanto organizativas, técnicas y de formación del capital humano, para

resguardar la integridad, confidencialidad y disponibilidad de los datos contenidos en sus registros con la finalidad de evitar la alteración, pérdida, transmisión y acceso no autorizado de los mismos.

_____

(1) Esta disposición comenzará a regir una vez que entre en vigencia la Ley N°21.180, sobre Transformación Digital del Estado.

Para ello, se propone a los órganos de la Administración del Estado, la implementación de las siguientes recomendaciones de seguridad de la información destinadas a la gestión de riesgos, mitigación de daños y resiliencia de sistemas y procesos de tratamiento de datos personales:

i) Garantizar en todo momento la seguridad de esta información, mediante el uso de sistemas informáticos actualizados y protegidos;
ii) Incorporar procedimientos para la prevención de filtraciones y accesos indebidos; y la definición de perfiles de acceso a los bancos de datos;
iii) Informar a los titulares de datos personales sensibles, de las eventuales brechas de seguridad que pudieran ocurrir, de las posibles consecuencias de estas vulneraciones y de las medidas de solución o resguardo adoptadas;
iv) En aquellos casos en que los datos recolectados sean comunicados o transmitidos a terceras personas, naturales o jurídicas, se recomienda la adopción de medidas de encriptación, a efectos de asegurar la integridad y confidencialidad de los datos entre remitente y destinatario.

Adicionalmente, los organismos públicos deben adoptar las medidas de seguridad establecidas en el artículo 11 y siguientes del decreto supremo N°83, de 2004, del Ministerio Secretaría General de la Presidencia, en lo relativo a establecer una política que fije las directrices generales orientadoras en materia de seguridad de bases de datos que se encuentran en su poder, que defina un encargado de seguridad al interior del servicio, mediante el correspondiente acto administrativo, y que a cada banco de datos se le asigne un responsable.

14. OBLIGACIONES EN CASO DE TRATAMIENTO DE DATOS PARA ENCUESTAS, ESTUDIOS DE MERCADO Y SONDEOS DE OPINIÓN.

De acuerdo con lo establecido en el artículo 3° de la ley N°19.628, cuando los órganos o servicios públicos recolecten datos personales a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que la ley regula, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información.

La comunicación de sus resultados debe omitir las señas que puedan permitir la identificación de las personas consultadas, debiendo sólo comunicarse los datos que tengan la calidad de estadísticos, es decir, los que, en su origen o como consecuencia de un tratamiento, no pueden ser asociados a un titular identificado o identificable, por haber sido aplicado a su respecto un procedimiento de disociación de datos.

Asimismo, el titular del dato puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión. Para ello se recomienda que el órgano o servicio informe al titular del dato, además de los aspectos señalados y al momento de realizarse la recopilación, que le asiste el derecho a oponerse, en cualquier tiempo, a la utilización de los mismos con los fines indicados.

15. RESPONSABILIDAD POR LAS INFRACCIONES Y DERECHO A INDEMNIZACIÓN.

De conformidad al artículo 23 de la ley N°19.628, el órgano de la Administración del Estado responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo con lo requerido por el titular o, en su caso, lo ordenado por el tribunal.

En cualquier caso, la indemnización respectiva será fijada prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos, y en el marco del procedimiento judicial legalmente aplicable en la especie.

16. DELEGADO DE PROTECCIÓN DE DATOS.

Para facilitar el cumplimiento de las obligaciones establecidas en la ley N°19.628 y una mejor observancia de las presentes Recomendaciones, se sugiere que las distintas autoridades, jefaturas o jefes superiores de los órganos o servicios de la Administración del Estado, designen a un funcionario o funcionaria de dicha repartición para desempeñarse como delegado o delegada de protección de datos y constituya un contacto efectivo en la materia con el Consejo para la Transparencia.

La designación y las comunicaciones que se establezcan para los efectos antedichos no alterarán, en caso alguno, la responsabilidad prevista en el artículo 23 de la ley N°19.628.

17. RECOMENDACIONES SOBRE PROTECCIÓN DE DATOS PERSONALES POR DISEÑO.

Si bien la Ley N°19.628 no contempla una regla especial que obligue implementar la protección de datos personales por diseño, y teniendo presente los principios de responsabilidad, eficiencia y eficacia en la Administración del Estado, el deber de velar por la eficiente e idónea administración de los medios públicos y por el debido cumplimiento de la función pública, todos contenidos en el decreto con fuerza de ley N°1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.575, orgánica constitucional de bases generales de la Administración del Estado; y el derecho fundamental a la protección de datos personales, se recomienda a los órganos de la Administración del Estado desarrollar e implementar sus sistemas de procesamiento bajo los siguientes principios que inspiran la protección de datos personales por diseño:

17.1. Principio de proactividad y prevención. Es recomendable que los órganos de la Administración del Estado diseñen, implementen y operen sus sistemas de procesamiento de datos personales identificando previamente los riesgos al derecho a la protección de datos personales de los titulares, propendiendo a una gestión adecuada, mediante su neutralización o mitigación.

17.2. Principio de protección predeterminada. Es recomendable que los órganos de la Administración del Estado proporcionen a los titulares de datos personales el más alto nivel de protección de sus datos por defecto y de manera automática en los sistemas de procesamiento de datos que desarrollen, implementen u operen.

17.3. Principio de protección desde el diseño. Es recomendable que los órganos de la Administración del Estado incorporen la protección de datos personales como un componente esencial e indispensable de los sistemas de procesamiento de datos personales que desarrollen, implementen u operen, desde su diseño.

17.4. Principio de funcionalidad total. Es recomendable que los órganos de la Administración del Estado comprendan sus sistemas de procesamiento de datos personales como sistemas funcionales eficaces y eficientes tanto respecto de su propósito principal (el cumplimiento de su mandato legal) como respecto del derecho constitucional a la protección de datos personales. Esto significa, entre otras cosas, que una aplicación sobre seguridad ciudadana debe ser eficiente y eficaz para ese propósito y a su vez, ser eficiente y eficaz en la protección de los datos personales. Se recomienda la existencia de reglas y mecanismos que permitan una coexistencia balanceada entre el resguardo y protección del derecho, y los objetivos de los mecanismos de procesamiento de datos.

17.5. Principio de seguridad punta a punta. Es recomendable que los órganos de la Administración del Estado protejan el ciclo completo del procesamiento de datos personales, desde su diseño, implementación y operación, adoptando las medidas necesarias para garantizar la seguridad de la información (integridad, confidencialidad y disponibilidad) como el uso de cifrado en todo momento, la anonimización temprana, la definición de roles de acceso a datos, la destrucción

segura de datos y el establecimiento de mecanismos para el ejercicio de los derechos de los titulares.

17.6. Principio de visibilidad y transparencia. Es recomendable que los órganos de la Administración del Estado adopten las medidas de transparencia necesarias respecto a sus sistemas de procesamiento de datos personales, informando a los titulares sobre la recolección, procesamiento, eventual comunicación y purga de datos, a través de políticas legibles de protección de datos personales y mecanismos de notificación a titulares.

17.7. Principio de enfoque centrado en el usuario. Es recomendable que los órganos de la Administración del Estado pongan en funcionamiento, en el nivel operacional, el mandato constitucional de tutela del derecho a la protección de los datos personales al momento de diseñar, implementar y operar un sistema de procesamiento de datos personales manteniendo un enfoque centrado en las personas. Esto significa que se deben adoptar sistémicamente las medidas necesarias para garantizar un efectivo control por parte del titular de los tratamientos de datos que se realicen y que le conciernan.".

2° Sustitúyase el texto de las recomendaciones sobre protección de datos personales por parte de los órganos de la Administración del Estado, publicado en el Diario Oficial con fecha 14 de septiembre de 2011, por el presente texto actualizado y refundido.

3° Publíquese la presente resolución exenta en el Diario Oficial, según lo dispuesto en la letra b) del artículo 48 de la ley N°19.880 y en la página web de esta Corporación, sin perjuicio de su difusión a la ciudadanía a través de otros medios y soportes.

Anótese, publíquese en el Diario Oficial y en la página web del Consejo para la Transparencia, particularmente en el apartado de "Actos y documentos publicados en el Diario Oficial" y archívese.- David Ibaceta Medina, Director General (S), Consejo para la Transparencia.